blackbeltsecure.com

July 2025

DIGITAL DEFENSE DIGEST

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

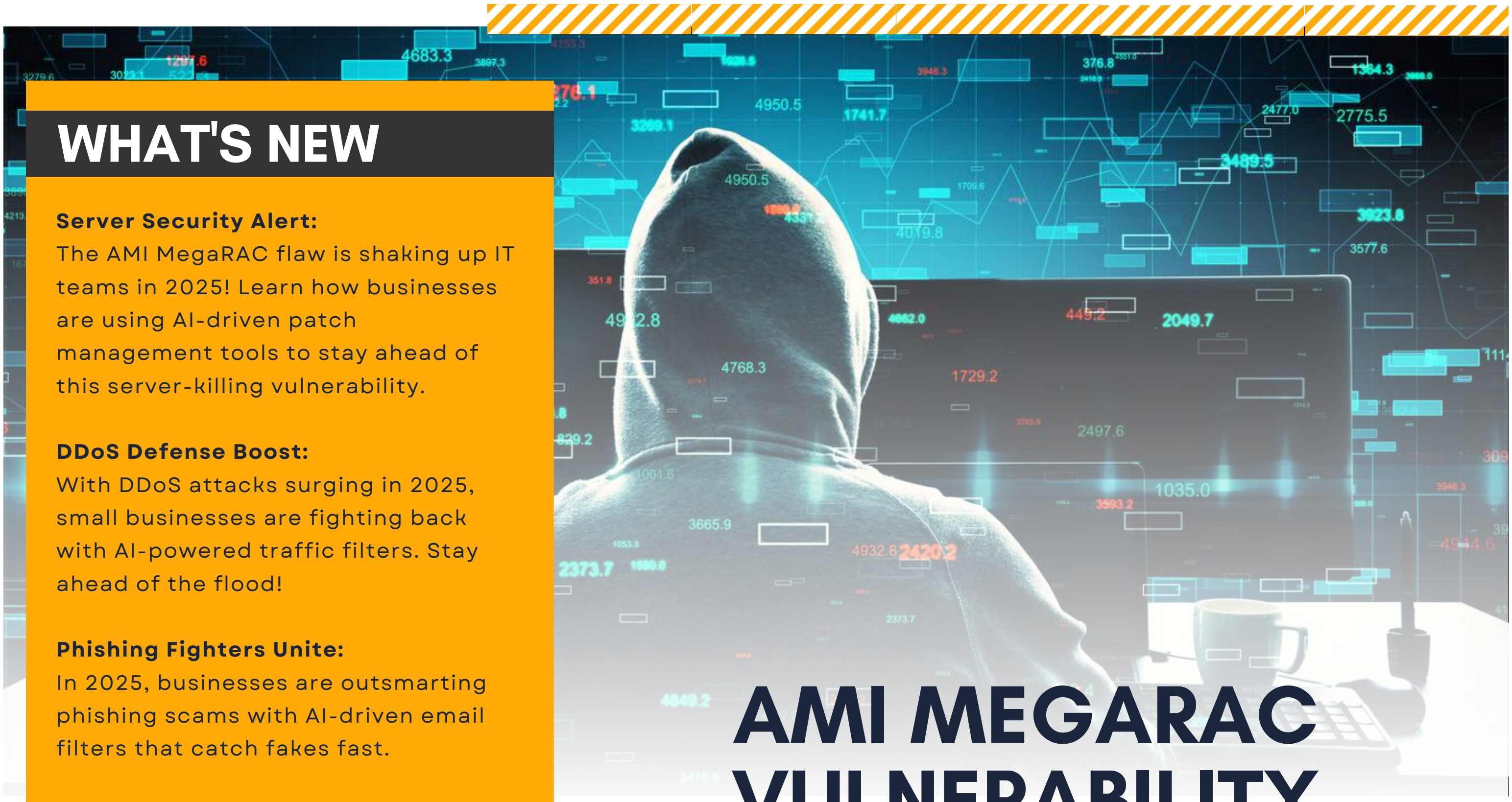
WHAT'S NEW

Server Security Alert:
The AMI MegaRAC flaw is shaking up IT teams in 2025! Learn how businesses are using AI-driven patch management tools to stay ahead of this server-killing vulnerability.

DDoS Defense Boost:
With DDoS attacks surging in 2025, small businesses are fighting back with AI-powered traffic filters. Stay ahead of the flood!

Phishing Fighters Unite:
In 2025, businesses are outsmarting phishing scams with AI-driven email filters that catch fakes fast.

Black Belt Secure offers comprehensive cybersecurity solutions to protect your personal and business data from online threats.



AMI MEGARAC VULNERABILITY

OUR SERVER SECURITY WAKE-UP CALL

A critical vulnerability (CVE-2024-54085, CVSS 10.0) in AMI MegaRAC Baseboard Management Controller (BMC) firmware is under active exploitation, threatening servers from vendors like AMD, Supermicro, and Fujitsu, according to CISA. This flaw in the Redfish interface allows attackers to bypass authentication, gaining full control to deploy malware, ransomware, or even cause physical server damage. Discovered in March 2025, patches are available, but applying them requires downtime, leaving many organizations vulnerable. Data centers and businesses with mission-critical servers are at high risk, as BMCs control everything from OS reinstallation to hardware settings, even when servers are off. The ease of exploitation and widespread use of AMI MegaRAC make this a top priority for IT teams.

Why It Matters

This vulnerability highlights the dangers of exposed management interfaces and the need for rapid patching. Unsecured BMCs can lead to catastrophic breaches, impacting operations and reputation.

What to Do

Implement "never trust, always verify" policies, requiring continuous authentication for vendor access.

- Check if your servers use AMI MegaRAC and verify patch status with vendors like HPE or Lenovo.
- Isolate BMC interfaces on dedicated networks to prevent public exposure.
- Engage Black Belt Secure for a vulnerability assessment to identify and mitigate risks.

This monthly publication is provided by Black Belt Secure

OUR MISSION:

To empower businesses of all sizes with the knowledge and tools they need to thrive in today's increasingly complex cyber threat landscape. We are dedicated to providing cutting-edge cybersecurity solutions and expert guidance to help our clients

DDOS ATTACKS SKYROCKET

IS YOUR INFRASTRUCTURE READY?

Cloudflare reported blocking 20.5 million DDoS attacks in Q1 2025, a 358% increase year-over-year, with one-third targeting its own network. These distributed denial-of-service attacks overwhelm servers with traffic, disrupting services and costing businesses downtime and revenue. Industries like finance, healthcare, and e-commerce are prime targets, as attackers exploit vulnerabilities in cloud infrastructure and IoT devices. The rise in attack volume reflects growing sophistication, with bad actors leveraging AI to amplify their efforts. Smaller organizations, often lacking robust defenses, face significant risks, as mitigation requires advanced infrastructure and real-time monitoring.

Why It Matters

DDoS attacks aren't just annoying—they can cripple your business, tank customer trust, and drain your bottom line. With attacks growing in scale and sophistication, no one's immune, especially businesses leaning on online services or cloud platforms. A single attack can knock out your website, disrupt transactions, and leave customers frustrated, while recovery costs and reputational damage pile up fast. Staying ahead means building a fortress around your infrastructure before the next wave hits.

What to Do

Get Protected

Deploy DDoS mitigation tools like Cloudflare, Akamai, or Fastly to filter out malicious traffic and keep your services online. These solutions use advanced algorithms to detect and block harmful requests, ensuring your website or application remains accessible even during high-volume attacks. They also provide scalable infrastructure to absorb and distribute traffic surges effectively.

Test Your Resilience

Run stress tests to see how your systems handle traffic spikes and shore up any weak links. Simulate real-world attack scenarios to identify vulnerabilities in your infrastructure, such as bottlenecks in bandwidth or server capacity, and optimize configurations to ensure your systems can withstand sudden surges without crashing.

Stay Vigilant

Set up real-time monitoring to catch suspicious traffic patterns early and respond before damage is done. Use tools like intrusion detection systems or network monitoring platforms to track anomalies, such as unusual spikes in requests or traffic from specific regions, enabling quick identification and mitigation of potential threats.

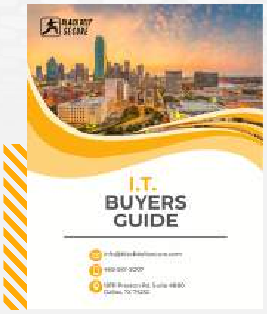
Call in the Experts

Work with Black Belt Secure to craft a bulletproof DDoS defense plan, complete with 24/7 monitoring and rapid incident response.

FREE REPORT DOWNLOAD:

IT Buyer's Guide

- The 3 most common ways IT services companies charge for their services, and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- 21 revealing questions to ask your IT support firm BEFORE giving them access to your computer network, email and data.



Claim Your FREE Copy Today At: blackbeltsecure.com/reports

OUTSMART PHISHING:

5 ESSENTIAL TIPS FOR YOUR TEAM

Phishing scams are the cyber equivalent of a wolf in sheep's clothing, and in 2025, they're sneakier than ever. Attackers are wielding AI-powered tricks like deepfake videos, hyper-personalized emails, and culturally tailored scams—like the "Wedding Invitation" Android phishing campaign that hit India hard—to trick users into handing over credentials or clicking malicious links. These attacks aren't just annoying; they can lead to massive data breaches, financial losses, and a trashed reputation for businesses, non-profits, and government agencies alike. With bad actors mimicking trusted contacts and crafting emails that look legit, even savvy users can get duped. The good news? You can outsmart these scammers with the right strategies. From training your team to spot red flags to locking down accounts with cutting-edge tools, here's how to keep phishing attacks at bay and protect your sensitive data from falling into the wrong hands. Let's make your business a fortress against these cyber con artists!

Why It Matters

Phishing is the gateway to many cyber disasters, from stolen credentials to ransomware infections. A single click on a malicious link can compromise your entire network, costing you time, money, and customer trust. With attackers getting craftier, businesses can't afford to skimp on defenses. Staying proactive with training and tech keeps your team one step ahead, ensuring your data stays safe and your reputation intact.

What To Do:

Train Employees Regularly

Conduct quarterly phishing simulations to teach staff to spot suspicious emails and links. These exercises mimic real-world phishing attempts, helping employees recognize red flags like misspelled domains or urgent language, fostering a security-conscious culture and reducing the likelihood of falling for scams.

Enable Multi-Factor Authentication (MFA)

Require MFA for all accounts to reduce the risk of credential theft. By adding an extra verification step, such as a code sent to a mobile device, MFA ensures that even if passwords are compromised, unauthorized access is significantly harder, enhancing overall account security.

Use Advanced Email Filters

Deploy AI-based filters to detect and block phishing emails before they reach inboxes. These filters analyze email content, sender behavior, and metadata to identify malicious patterns, automatically quarantining threats and reducing the chance of employees interacting with dangerous emails.

Verify Sender Authenticity

Teach employees to check email domains and avoid responding to unsolicited requests. Training should emphasize scrutinizing sender addresses for subtle discrepancies (e.g., "exampl3.com" vs. "example.com") and avoiding clicking links or sharing sensitive information without verifying the source's legitimacy.

Monitor for Anomalies

Use security tools to flag unusual login attempts or email patterns, catching attacks early. Implement solutions that track login locations, times, or email sending behaviors, alerting administrators to suspicious activities like multiple failed logins or mass emails from a compromised account, enabling rapid response to potential threats.

By prioritizing these steps, you can reduce phishing risks and protect sensitive data. Black Belt Secure's managed detection and response services can further bolster your defenses with 24/7 monitoring.

Don't let phishing scams catch you off guard. Contact Black Belt Secure for a free phishing risk assessment and tailored employee training programs. Get Protected!

CARTOON OF THE MONTH

"If you could fill out the attached survey that would really help me out."

TRIVIA

Summer brings travel, but what's the top cybersecurity risk for business travelers in 2025?

A. Public Wi-Fi attacks
B. Phishing emails
C. Lost devices
D. Malware downloads

Answer: A. Public Wi-Fi attacks spike in summer, with 250,000 incidents reported, per Verizon's 2025 Data Breach Report.

SECURE YOUR SUPPLY CHAIN:

5 TIPS TO MANAGE VENDOR RISKS

Third-party vendors are a growing cybersecurity risk, as seen in recent supply chain attacks like the North Korean campaign embedding 35 malicious npm packages. Weak vendor security can expose your systems to breaches, as vendors often access sensitive data or infrastructure. With regulations like the EU's DORA and the US SEC's cybersecurity rules tightening in 2025, businesses must prioritize vendor management to avoid compliance violations and costly incidents. Here's how to secure your supply chain:

Vet Vendors Thoroughly

Assess vendors' cybersecurity posture using standardized frameworks like NIST or CIS controls.

Require Regular Audits

Mandate periodic security audits and penetration testing for all third-party partners.

Use Zero Trust Principles

Implement "never trust, always verify" policies, requiring continuous authentication for vendor access.

Monitor Vendor Activity

Deploy tools to track vendor interactions with your systems and flag anomalies in real time.

Contractual Safeguards

Include cybersecurity clauses in vendor contracts, specifying compliance and incident response requirements.

CYBERSIDE CHAT

Fortify Your Defenses: DDoS Protection Done Right

Protecting your systems from DDoS attacks is non-negotiable in 2025. Deploy tools like Cloudflare or Akamai to filter malicious traffic and keep services online. Stress-test your infrastructure to spot weaknesses and ensure it can handle sudden spikes. Real-time monitoring catches suspicious patterns early, while partnering with experts like Black Belt Secure delivers a tailored defense plan with 24/7 support to minimize downtime.

MFA: Your Extra Lock on the Digital Door

Enabling Multi-Factor Authentication (MFA) adds a critical layer of security to all accounts. By requiring a second verification step, like a texted code, MFA stops hackers in their tracks even if they snag your password, keeping your sensitive data safe.

Stay Sharp with Anomaly Monitoring

Using security tools to detect unusual login attempts or email patterns is like having a digital watchdog. Flagging oddities, such as logins from unfamiliar locations or sudden email spikes, lets you catch and stop attacks early, minimizing damage.